PROTECTING THE PUBLIC:
Office of Thrift Supervision's Control Over Computers Is Adequate

OIG-02-117 **September 11, 2002**

Office of Inspector General

****

The Department of the Treasury

Contents

Abbreviations

FY	Fiscal Year
OIG	Office of Inspector General
OTS	Office of Thrift Supervision

September 11, 2002

James E. Gilleran
Director
Office of Thrift Supervision

We conducted an audit of the Office of Thrift Supervision's (OTS) control over selected property items that, if lost or stolen, might compromise national security, the public's safety, or ongoing investigations. Sensitive property at OTS included computers only. Based on our audit, we judged that the risk that this property item could be lost or stolen was low. OTS had written guidance for managing computers and physical controls limiting access to this item. It also conducted physical inventories in a manner that was independent of the custodial function.

We conducted this audit at the request of Senator Charles E. Grassley, member of the Senate Committee on Finance. Our specific objectives were to answer the following questions:

1. Are Treasury's inventory regulations sufficient to prevent loss or theft of its inventory?
2. Which Treasury bureaus are most susceptible to inventory loss or theft and why?
3. Have any Treasury inventory items been identified as lost or stolen within the last 3 fiscal years?
4. Does Treasury have a sufficient plan to recoup inventory that cannot be located?

The audit fieldwork was performed from February to August 2002. We interviewed OTS officials and evaluated records and procedures. The scope of the review covered FY 1999 to FY 2001. See Appendix 1 for a more detailed description of the audit objectives, scope, and methodology.

Results in Brief

OTS reported seven computers lost or stolen during fiscal years (FY) 1999 through 2001, having a total acquisition cost of $20,214. Our assessment of the risk that computers could be lost or stolen was low (●).[1] OTS had written guidance, directives, and procedures for managing and safeguarding computers. It also required reporting and investigation of all lost or stolen computers. OTS conducted periodic physical inventories of its property that were independent of the custodial function. Based on the information developed during our audit, we did not make any recommendations in this report.

Background

OTS is responsible for chartering, examining, supervising, and regulating federal savings associations and federal savings banks. OTS also examines, supervises, and regulates state-chartered savings associations and provides for the registration, examination, and regulation of savings association affiliates and holding companies. OTS is headquartered in Washington, DC and has four regional offices in: Jersey City, New Jersey; Atlanta, Georgia; Dallas, Texas; and San Francisco, California.

Results of Audit

● OTS Control Over Computers

For FY 2001, OTS reported that it had 1,627 computers (828 desktops and 799 laptops). It also reported that seven laptop computers, having a total acquisition cost of $20,214, had been lost or stolen during the audited period. Subsequent investigations did not find any employees financially liable for the missing computers. We judged the risk of loss or theft of computers to be low. OTS had a large number of computers dispersed throughout the country. This factor increased the risk of loss or theft. However, OTS had (1) written policies and procedures, and (2) conducted and documented annual physical inventories of all

[1] Office of Inspector General (OIG) judgment (● Low ● Moderate ● High)

computers. These factors reduced the risk of loss or theft. In addition, OTS had controls that limited access to computer files and OTS' computer network. These controls decreased the risk that sensitive data would be compromised, even if a computer were lost or stolen.

Geographic distribution of computers

OTS personnel were assigned computers to use in the performance of their duties. Examiners often used their computers in the field (off-site). A large number of computers dispersed over numerous geographic locations, many of which were carried in the field, increased the risk that some of those items would be lost or stolen. Since OTS' mission made it impractical to reduce the number of computers or centralize their location, it was important that a strong control environment be in place.

Written policies and procedures

OTS had written policies that provided guidance on the control and management of computers. These policies included conducting physical inventories; reporting lost or stolen items; determining employee accountability; obtaining computers from departing employees; and disposing of excess computers.

Physical inventories

OTS conducted and documented annual physical inventories of all computers. Items were scanned into the automated tracking system using a scanner. Discrepancies found during the scanning process were reported to the appropriate offices for investigation. We reviewed recent physical inventory reports and observed that OTS offices and headquarters property management personnel followed up on any reported discrepancies

Data security

OTS had sensitive but unclassified information.[2] Accessing OTS computer systems required access rights and a related password. All users of OTS information technology resources receive annual security training. OTS used a commercially available computer program to sanitize its computer hard disks before the machines left OTS custody. After the hard drive had been sanitized, OTS procedures require that an independent person verify the effectiveness of the purge.

These controls over data security decreased the risk that sensitive information would be compromised, even if a computer was lost or stolen.

Reporting, investigating, and recouping lost or stolen computers

OTS employees were required to report lost or stolen computers assigned to them. During the audited period, seven laptop computers were reported lost or stolen. The total acquisition cost of these computers was $20,214. The circumstances associated with these cases are summarized below:

Circumstance of Loss or Theft	Number of Computers
Stolen from a hotel room	2
Lost during transfer between OTS units	1
Reason Not Identified	4
Total	7

Local police departments investigated the two hotel room losses. On-site OTS staff investigated the remaining losses. No employee was disciplined or held financially responsible for any of the lost or stolen computers.

[2] OTS defined sensitive but unclassified information as information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

* * * * * * *

We appreciate the cooperation we received from OTS officials during this audit. If you wish to discuss this report, you may contact me at (312) 886-6300, ext. 118.

/s/
Roberta N. Rickey
Regional Inspector General for Audit

The overall objective of this audit was to address concerns Senator Charles E. Grassley, member of the Senate Committee on Finance, raised regarding Treasury-wide inventory practices for items that if lost or stolen, might compromise the public's safety, national security, or ongoing investigations. Our specific objectives were to answer the following questions:

(1) Are the bureau's policies and practices sufficient to prevent loss and theft?
(2) What items have been lost or stolen during FY 99 – 01?
(3) Does the bureau have a sufficient plan to recoup lost items?
(4) What improvements can be made to prevent future losses?

At the OTS, we considered computers to be a sensitive property item. Our audit scope covered FY 1999, 2000, and 2001 (from October 1, 1998 through September 30, 2001). To accomplish our objectives, we requested data on inventory levels at or near the end of FY 2001[3] and computers reported lost/stolen during FY 1999 – FY 2001; reviewed pertinent laws and regulations; reviewed written bureau policies; reviewed the latest physical inventory reports; and reviewed information related to lost/stolen computers.

To assess the risk of loss or theft of sensitive items, we examined elements related to six factors: Policies, Physical Controls, Inventory Records, Physical Counts, Quantity, and Threat.

Policies - establish management guidelines and standards.
Physical Controls - limit access.
Property Records - identify accountability.
Physical Counts - assure reliability of records.
Quantity - impacts the opportunity for loss or theft.
Threat - includes ease of loss and harm of unauthorized use.

Having weighed these factors and the resulting overall control environment, we assigned a risk factor of low (●), moderate (●), or high (●).

[3] The date of the reported inventory levels for the computers was from August 2001.

We conducted our audit between February to August 2002 in accordance with generally accepted government auditing standards.

Central Region

Roberta N. Rickey, Regional Inspector General
Charles Allberry, Audit Manager
Bradley Mosher, Audit Manager
Claire Schmidt, Auditor

Department of the Treasury

Office of the Under Secretary of the Treasury for Enforcement
Office of the Assistant Secretary of the Treasury for Management/Chief Financial Officer
Office of Strategic Planning and Evaluations Management Control Branch
Office of Accounting & Internal Control
Office of Organizational Improvement

Office of Thrift Supervision

Director
Special Counsel
Internal Review Analyst

Office of Management and Budget

OMB Budget Examiner